ABSTRACT OF THE DISCLOSURE

A method and apparatus for protecting secured files stored on a file system employs a file security status associated with each file to signal whether or not access to the file is allowed. The file security status is stored in a fixed location in memory. Upon opening the associated file, the file security status is copied to a second location in memory. Depending upon the file security status stored in the second location, operations on the file by a client are either allowed or denied. Operations on non-secure files are always allowed. Operations on secured files are allowed only after verification of the client's authorization to access the file and the subsequent modification of the file security status stored in the second memory location. The method protects secured files from deletion by unauthorized clients. This is accomplished by, upon opening a secure file, initializing a third memory location to a value indicating that the file will not be deleted upon closing. This value may be changed by an authorized client only after going through the above-described verification process. Once the value has been changed to reflect that the file should be deleted when closed, the file will be deleted when closed. A method for creating a new secure file is also provided.